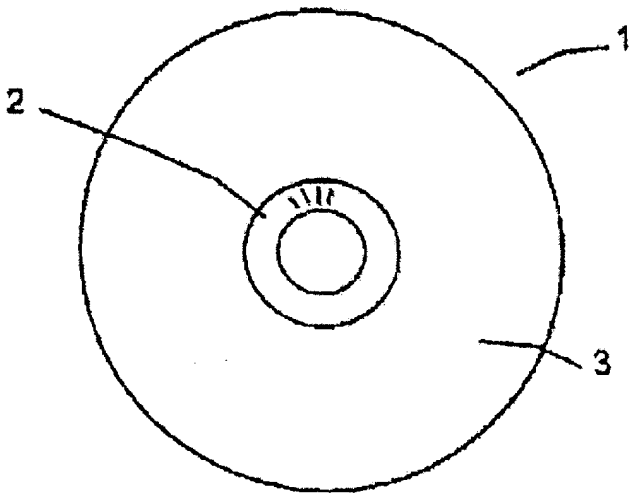
COPYING PREVENTION DEVICE AND METHOD

Publication number: JP2000076141
Publication date: 2000-03-14
Inventor: MORIFUJI HAJIME; YOSHIURA YUTAKA
Applicant: HITACHI LTD
Classification:
- international: ***G06F12/14; G06F21/24; G11B20/00; G11B20/10;*** *G06F1/00;* **G06F12/14; G06F21/00; G11B20/00; G11B20/10;** G06F1/00; (IPC1-7): G06F12/14
- European: G11B20/00P
Application number: JP19990091260 19990331
Priority number(s): EP19980307028 19980902

Also published as:
EP0984346 (A1)
US6782190 (B1)

Abstract of **JP2000076141**

PROBLEM TO BE SOLVED: To protect digital data on a data storage medium from unauthorized copying even when copying prevention information inside the data is forged. SOLUTION: Copying protective device and method to be used in a digital data recorder like a DVD-RAM include the use of a DVD disk 1 provided with a unique serial number stored in the read-only part 2 of a disk for data recording. The serial numbers of the respective disks are digitally signed together with other copying control information. The digital signature is verified in a DVD player/recorder and whether or not the disk to be reproduced is an original disk or a proper copy is checked. When it is not either one, the reproduction recording of the data of the disk are blocked. A copying generation management system is executed by the use of the copying control information as well.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－76141
（P2000－76141A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ

審査請求　未請求　請求項の数23　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－91260

(22)出願日　平成11年３月31日(1999.3.31)

(31)優先権主張番号　９８３０７０２８．５

(32)優先日　平成10年９月２日(1998.9.2)

(33)優先権主張国　ヨーロッパ特許庁（ＥＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　森藤　元
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

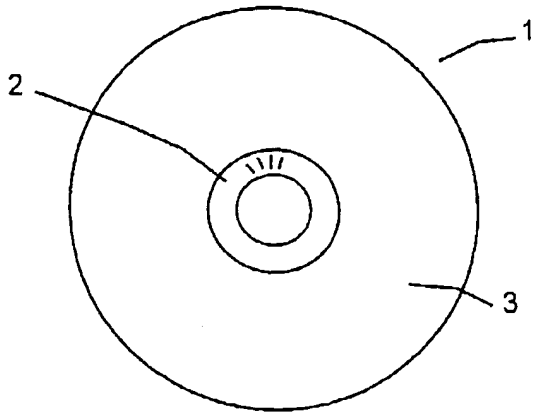
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　100087170
弁理士　富田　和子

(54)【発明の名称】　コピー防止装置および方法

(57)【要約】
【課題】データ記憶媒体上のデジタルデータは、データ内のコピー防止情報が偽造されたものであっても、不正なコピーから保護する。
【解決手段】データ記録用のディスクの読み出し専用部分２に記憶された一意なシリアル番号を有するＤＶＤディスク１を用いることを含む、ＤＶＤ－ＲＡＭのようなデジタルデータレコーダで使用するコピー保護装置および方法である。各ディスクのシリアル番号は他のコピー制御情報とともにデジタル的に署名される。このデジタル署名はＤＶＤプレーヤ／レコーダ１３、３０にて検証され、再生しようとしているディスクがオリジナルディスクかあるいは正当なコピーかをチェックする。いずれでもなければ、そのディスクのデータの再生および記録が阻止される。コピー制御情報の使用によっても、コピー生成管理システムを実施することができる。

図1



【特許請求の範囲】
【請求項１】媒体識別子を有する記憶媒体上に記憶されたデータを処理する装置であって、前記媒体識別子と、前記媒体上に記憶された媒体識別子の検証情報との関係に依存した記憶データの処理を制御する手段を有する装置。
【請求項２】請求項１記載の装置であって、前記媒体識別子は前記媒体の読み出し専用部分に記憶される装置。
【請求項３】請求項１または２記載の装置であって、前記媒体識別子は、第１の媒体識別子を有し、前記検証情報は第２の媒体識別子を有する装置。
【請求項４】請求項３記載の装置であって、制御手段は前記第１および第２の媒体識別子の比較に応じて動作する装置。
【請求項５】請求項４記載の装置であって、前記制御手段は、前記第１および第２の媒体識別子が異なる場合、データの再生を阻止する装置。
【請求項６】請求項４または５記載の装置であって、前記制御手段は、前記第１および第２の媒体識別子が異なる場合、データの記録を阻止する装置。
【請求項７】先行する任意の請求項に記載の装置であって、さらに、前記検証情報を認証するための手段を有する装置。
【請求項８】請求項７記載の装置であって、前記検証情報はデジタル署名され、前記認証手段は、このデジタル署名を検証する手段を有する装置。
【請求項９】先行する任意の請求項に記載の装置であって、さらに、媒体からのデータの記録を制御する手段を有する装置。
【請求項１０】請求項９記載の装置であって、前記記録制御手段は、媒体上に記憶されたコピー管理データに応じて動作する装置。
【請求項１１】請求項１０記載の装置であって、前記コピー管理データは、媒体が自由にコピーできること、１回だけコピーできること、またはコピーできないことを指定する装置。
【請求項１２】請求項１０または１１記載の装置であって、前記コピー管理データはデジタル的に署名される装置。
【請求項１３】先行する任意の請求項に記載の装置であって、ＤＶＤプレーヤを構成する装置。
【請求項１４】請求項１３記載の装置であって、前記媒体はＤＶＤディスクからなる装置。
【請求項１５】媒体識別子およびこの識別子の検証情報が記憶された記憶媒体上に記憶されたデータを処理する方法であって、前記媒体上に記憶された前記媒体識別子と媒体識別子の検証情報との関係に依存して前記記憶データの処理を制御することを含む方法。
【請求項１６】媒体識別子を有するデータ記憶媒体上にデータを記録する記録装置であって、前記媒体識別子の検証情報を生成する手段を有し、前記検証情報は前記媒体上に記憶される装置。
【請求項１７】請求項１６記載の装置であって、前記検証情報をデジタル的に署名する手段を有する装置。
【請求項１８】請求項１６または１７記載の装置であって、前記検証情報は媒体識別子を含む装置。
【請求項１９】請求項１６から１８のいずれか１つに記載の装置であって、そこからデータが記録されようとしている記録元の媒体上に記憶されたコピー管理データに応じて、媒体上への記録を制御する手段を有する装置。
【請求項２０】媒体識別子を有するデータ記憶媒体上へデータを記録する方法であって、前記媒体上に記憶されるべき媒体識別子の検証情報を生成することを含む方法。
【請求項２１】請求項２０記載の方法であって、前記媒体の読み出し専用部分から前記媒体識別子を読み出すことを含む方法。
【請求項２２】請求項２０または２１記載の方法であって、デジタル署名を用いて前記検証情報を保護することを含む方法。
【請求項２３】媒体上に記憶された媒体識別子およびこの識別子の検証情報を有するデータ記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コピー防止に関し、特に（但し、排他的にではなく）、データ記憶媒体上のデジタルデータを不正な(unauthorised)コピーから保護するための装置および方法に関する。
【０００２】
【従来の技術】オーディオＣＤやＣＤ－ＲＯＭのようなデジタル媒体によれば、それらに記憶されたデジタルデータを完全に複製(reproduction)することができるが、従来、これらの媒体は通常読み取り専用であるため、侵害の可能性のある者は高品質のコピーを作製するためには記録専門家およびＣＤプレス機器を必要とすることから、不正な複製を取り締まる問題はある程度緩和された。
【０００３】しかし、広く利用される低コストのレコーダを作製することを目的とした、ＣＤ－Ｒ（ライトワンス）やＣＤ－ＲＷ（書き換え可能）を含む記録可能デジタル記憶技術、並びにデジタル汎用ディスク(DVD: Digital Versatile Disk)技術の消費者市場への導入に伴って、大規模な海賊行為を防止するために高度なコピー防止システムの必要性が増大してきた。ＤＶＤ－ＲＡＭレコーダとして知られているＤＶＤレコーダは、究極的には、コンピュータハードディスクおよびビデオカセットレコーダを含む、現在利用可能な種々の異なる形式の記憶装置にとって代わると予想される。
【０００４】ＤＶＤ技術の原理は、市販の日立製作所製ＧＦ－１０００シリーズのようなＤＶＤ－ＲＡＭについ

て十分に確立されている。ＤＶＤ原理の詳細情報については、McGraw-Hill社から出版されたJim Taylor著"DVD Demystified"を参照されたい。

【０００５】何らかのコピー管理(copy control)なしには、ＤＶＤディスクやＣＤ－ＲＯＭで頒布される映画、オーディオ記録および他のデジタルコンテンツは、記録可能なＤＶＤ－ＲＡＭのようなデジタルデータ記憶媒体に対してＤＶＤ－ＲＡＭや他のデジタルレコーダにより容易に記録することが可能であり、このデジタル記録媒体から、当該データをコピー品質の劣化なしに他のＤＶＤディスクに対して多数回コピーすることができる。

【０００６】不正なコピーを阻止するために、消費者に販売されている装置にはコピー防止機構が内蔵されている。例えば、Jim Taylor著"DVD Demystified"の第１２８頁に記載されているように、ＤＶＤディスクのデータセクタ内にコピー管理信号を埋め込むことができる。このような埋め込み情報を用いるコピー管理の可能な方法は、デジタルコンテンツの提供者がそのデータに"ネバーコピー(Never-Copy)"フラグを埋め込んで、例えばＤＶＤ－ＲＯＭディスクのような読み出し専用媒体で、映画や他のデジタルコンテンツを供給するものである。ＤＶＤプレーヤ／レコーダはこのフラグの存在をチェックし、もしフラグがある場合にそのディスクをコピーしようとすると、記録回路は記録を阻止する。しかし、この種のコピー防止策は、コンピュータ用周辺機器としてのＤＶＤ－ＲＯＭ／ＲＡＭデバイスを用いることにより回避することができる。これにより、記録可能ディスク上に、コピー防止情報を含めて、オリジナルディスクからデータをビット単位に記録することができる。

【０００７】このようなコピー防止法の回避を防止するために、ＤＶＤプレーヤには、ＲＯＭディスクと異なり、記録可能なディスク上にネバーコピーフラグがあるか否かをチェックするよう設計されたものがある。このような記録可能なディスク上のフラグの存在は、そのディスクがオリジナルのＲＯＭディスクを不正にコピーしたものであることを示し、その結果、そのディスク上のデータの再生が阻止される。他方、ＲＯＭディスクが使用されていることをそのプレーヤが検知した場合には、そのディスク上のデータを再生する。

【０００８】

【発明が解決しようとする課題】しかし、ディスクをコピーするコンピュータユーザはネバーコピーフラグを含めたデータのすべてをビット単位にコピーするという前提の下で、この方法は機能する。コピー管理情報がオリジナルＲＯＭディスク上のどこに位置しているかを認識し、または突き止めて、このオリジナルディスクを記録可能なディスク上にコピーする際に、当該情報を変更または上書きすることのできるコンピュータユーザによれば、上記方法は依然容易に回避されうる。

【０００９】上記防止法の他の問題は、それに柔軟性がなく、コピーが許可される程度を管理するコピー生成管理システム(copy generation management system: CGMS)を設ける方法が存在しないことである。

【００１０】例えば、オリジナルのデータ記憶媒体の内容をバックアップ媒体にコピー可能としながら、そのバックアップ媒体から更に別のコピーの生成は阻止するような方法が存在しない。

【００１１】本発明は、このような問題に対処することを目的とする。

【００１２】

【課題を解決するための手段】本発明によれば、媒体識別子を有する記憶媒体上に記憶されたデータを処理する装置が提供される。この装置は、媒体上に記憶された媒体識別子と、媒体識別子の検証情報との関係に依存した記憶データの処理を制御する手段を有する。

【００１３】前記媒体識別子は第１の媒体識別子であり、前記検証情報は第２の媒体識別子からなり、前記装置は、第１および第２の媒体識別子が異なる場合に、再生または記録を阻止することができる。

【００１４】オリジナルディスクの場合、第２の媒体識別子は第１の媒体識別子のコピーであってもよい。

【００１５】本装置は、検証情報を認証する手段を有してもよい。検証情報は、例えばデジタル署名され、認証手段はデジタル署名を検証する手段を有する。

【００１６】本発明はさらに、媒体上に記憶された媒体識別子および識別子の検証情報を有する記憶媒体に記憶されたデータを処理する方法を提供する。この方法は、媒体識別子と検証情報との関係に依存して記憶データの処理を制御することを含む。

【００１７】本発明は、媒体識別子を有するデータ記憶媒体上にデータを記録するための記録装置も提供する。この装置は、媒体上に記憶されるべき、媒体識別子の検証情報を生成する手段を有する。

【００１８】記録装置は、データがそこから記録されている記録元の媒体上に記憶されたコピー管理データに応じて、媒体上への記録を制御する手段を有してもよい。

【００１９】本発明は、さらに、媒体識別子を有するデータ記憶媒体上へデータを記録する方法を提供する。この方法は、媒体上に記憶されるべき媒体識別子の検証情報を生成することを含む。

【００２０】本発明によれば、さらに、媒体上に記憶された媒体識別子および媒体識別子の検証情報を有するデータ記憶媒体が提供される。

【００２１】本発明によれば、有利なことに、データ記憶媒体上のデジタルデータは、データ内のコピー防止情報が偽造されたものであっても、不正なコピーから保護することができる。また、この防止法は、バックアップコピーのような合法的なコピーの生成を可能とする。

【００２２】

【発明の実施の形態】以下、本発明の実施形態を、添付

の図面を参照しながら例示説明する。

【００２３】図１において、本発明によるＤＶＤディスク１は、識別子領域２とデータ領域３とを有する。識別子領域はディスクの読み出し専用部分に位置するので、ディスクの製造者のみがディスク１の製造時にこの領域に情報を書き込むことができる。例えば、識別子領域２はＤＶＤディスクのバーストカット領域(burst cutting area)でありうる。さらなる詳細はJim Taylor著"DVD Demystified"の第１２５～１２６頁を参照されたい。

【００２４】図２において、まず未記録（ブランク）ＤＶＤディスク４が媒体製造器５により従来の製造工程により製造される。ＤＶＤ媒体の製造工程はＣＤ－ＲやＣＤ－ＲＷディスクを製造するのに利用される工程と同様である。例えば、コンピュータ稼働シリアル番号生成ソフトウェアである媒体識別子発生器６は、例えばシリアル番号である固有の（一意な）識別子を生成する。この固有の識別子は、媒体識別子プリンタ７によりブランクＤＶＤディスク４のバーストカット領域２に書き込まれ、これにより、データ書き込みが可能なブランクＤＶＤディスク１が製造される。媒体識別子プリンタ７は、例えば、レーザ構成で、バーストカット領域２にストライプ状の一連のバーコードを刻むことによりシリアル番号を表す。実際上、この識別子は固有であるに越したことはないが、このことは必須ではない。重要なのは、広範なコピーを阻止するために、消費者が同一の識別子番号を持ったディスクを容易に入手できるという状況が殆ど起こりそうにないということである。

【００２５】ＤＶＤディスク１のデータ領域３へのアクセス可能性は、関与するディスクの型に依存する。ＤＶＤ－ＲＯＭディスクの場合、この領域は読み出し専用である。ＤＶＤ－ＲＯＭディスクは、Jim Taylor著"DVD Demystified"の第１２１～１２３頁に記載されているように、マスターコピーからそれを刻印（スタンプ）することにより生成することができる。これは、大量のディスクを製造する場合に最も費用効率のよい工程である。ＤＶＤ－ＲＯＭディスクの他の製造技術によれば、個々のディスクに対して固有のデータを内容させることができる。

【００２６】ＤＶＤ－Ｒ（ライトワンス）ディスクの場合、製造者は、識別子領域２内に例えば固有のシリアル番号を有するブランクディスクを製造する。但し、データ領域３は、コンテンツ供給者により、従来のデータ書き込み装置を用いて、一度だけ書き込みを行うことができる。一旦、コンテンツ供給者がディスクにデータを書き込むと、そのディスクは実質的にはＤＶＤ－ＲＯＭと同様に機能し、消費者が再書き込みを行うことはできない。

【００２７】また、ディスク１はＤＶＤ－ＲＡＭ（再書き込み可能）ディスクでありうる。これは、典型的には、消費者が記録および再記録できるブランクディスクとして頒布される。

【００２８】消費者へ頒布するための記録済みディスクの製造の背景にある原理については、ＤＶＤ－Ｒディスク１を参照して以下に説明する。このディスクは、例えば図２に示した製造構成で製造される。その結果、このディスク製造者からブランクディスクをコンテンツ供給者が受け取る。各ブランクディスクには、製造段階で、固有のディスク識別子、例えばシリアル番号が識別子領域２に書き込まれている。コンテンツ供給者は、ついで、映画、オーディオデータ、または他のデジタルコンテンツ（ここでは総称してデータと呼ぶ）、およびディスク１の他の関連情報（図３に示した記録装置８を参照して説明する）を記録することができる。

【００２９】コンテンツ供給者により使用されるべき記録装置８の一例は、ＤＶＤディスク１の読み出し専用部分２からディスク識別子を読み出す読み出し装置９と、コピー管理情報（ＣＣＩ）生成器１０と、この生成されたコピー管理情報をデータアーカイブ１２からのデータとともにディスク１上に記録する記録モジュール１１とを有する。

【００３０】記録装置８の動作を示す図４において、ステップｓ１で、読み出し装置９が記録中のディスク１からディスク識別子を読み出し、この識別子をＣＣＩ生成器１０へ渡す。ＣＣＩ生成器１０は、このディスク識別子の検証情報を、コピー管理情報として生成する（ｓ２）。ステップｓ３では、記録モジュール１１がデータアーカイブ１２からデータを読み出し、これを、ＣＣＩ生成器１０からのコピー管理情報とともにディスク１上に記録する（ｓ４）。こうして得られた記録済みディスク１はここではオリジナルディスクと呼ぶ。

【００３１】図５において、本発明によるＤＶＤプレーヤ１３は、読み出し装置１４と、ＣＣＩ検証モジュール１５と、再生装置１６とを有する。プレーヤ１３の動作を示す図６において、ステップｓ５では、読み出し装置１４が再生しようとしているディスク１からデータ、コピー管理情報およびディスク識別子を読み出し、この情報をＣＣＩ検証モジュール１５へ送る。ステップｓ６では、検証モジュール１５がコピー管理情報を検証しようとする。すなわち、コピー管理情報およびディスク識別子から、再生しようとしているディスクがオリジナルディスクか許可されたコピーかあるいは不正なコピーかを判定する。検証結果に問題がなければ、制御はステップｓ７へ進み、再生装置１６がデータを再生する。検証結果に問題があれば、制御はステップｓ８へ進み、再生が阻止される。なぜなら、検証処理が失敗したことは、読み出そうとしているディスクが不正コピーであることを意味するものと理解されるからである。

【００３２】ここで説明する本発明のすべての例において、読み出しモジュール１１、読み出し装置９，１４および再生装置１６のような、ＤＶＤディスクに対してデ

ータを読み書きするに要する装置は、日立製作所製ＧＦ－１０００シリーズのような市販のＤＶＤプレーヤ／レコーダにおいて現在使用されているような従来の回路で実施することができる。ＣＣＩ生成器１０およびＣＣＩ検証器１５のような、本発明を実施するために必要なブロックの機能は、従来のマイクロプロセッサを基本として回路上でソフトウェアによって実施することができる。

【００３３】ディスク１上に記録できるコピー管理情報の一例は、記録装置８内の読み出し装置９で読み出されるオリジナルディスク識別子の単なるコピーである。図７において、ステップｓ９では、読み出し装置９がオリジナルディスクからディスク識別子Ｓdを読み出し、ステップｓ１０で、Ｓdをコピー管理情報として保存する。ステップｓ１１では、記録モジュール１１がデータアーカイブ１２からデータを読み出して、このデータおよびＳdをディスク１のデータ領域３へ記録する（ｓ１２）。ステップｓ１３では、再生しようとしているディスクのディスク識別子であるＳｐを、プレーヤ１３内の読み出し装置１４がディスク１のバーストカット領域２から読み出し、これをＣＣＩ検証器１５へ送る。読み出し装置１４はまた、コピー管理情報すなわちＳdをディスク１のデータ領域３から読み出す。ステップｓ１４では、ＣＣＩ検証器１５が実際のディスク識別子Ｓｐをオリジナルディスク識別子Ｓdのコピーと比較する。もしオリジナルディスクがコピーされたのでなければ、２つの識別子、例えば、各ディスクのシリアル番号が同一となり、そのディスクが再生可能であることを示す信号が再生装置１６へ送られる（ｓ１５）。一方、オリジナルディスクがコピーされたのであれば、すなわち、オリジナルディスク上のすべてのデータが新たなディスクへ転送されたのであれば、新たなディスクのバーストカット領域２内のディスク識別子Ｓpは、新たなディスクのデータ領域３にコピーされたオリジナルディスク識別子Ｓdと異なることになる。この場合、そのディスクは不正にコピーされたものであり、再生できないという信号が再生装置１６へ送られる（ｓ１６）。

【００３４】コピー管理情報としてオリジナルディスク識別子のコピーを用いることは、前述したネバーコピーフラグの使用と同様の再生コピー管理の一形式を提供する。したがって、オリジナルディスクのコピーの作成自体は阻止されないが、この例によるＤＶＤプレーヤは当該コピー上のデータを再生しない。しかも、コピーされたディスクから第２世代のコピーを生成すること自体は、ステップｓ１４～ｓ１６で説明したようなプレーヤ１３と同じ検証チェックを行うことにより阻止される。これが機能するのは、ＳpがＳdと異なる場合のコピーを、第１世代のコピーであると記録装置が認識して、更なる記録を阻止することができるからである。

【００３５】上述のコピー管理方法によるコピー防止を消費者が回避することを禁止するために、コピー管理情報自体はアクセスや変更から保護される必要があると考えられる。

【００３６】適切な形式の保護の一例は、公開鍵暗号システムを基礎とすることができるデジタル署名を使用するものである。デジタル署名の形成方法は周知であり、デジタル署名ソフトウェアは、例えば、米国カリフォルニア州にあるＲＳＡデータセキュリティ社から市販されており、これは周知のＲＳＡ公開キーアルゴリズムを用いるものである。公開鍵システムの原理およびそのデジタル署名への使用について以下に説明する。より詳細な説明は、Bruce Schneier, "Applied Cryptography", John Wiley &; Sons, Inc. 1996, ISBN 0-471-11709-9を参照されたい。

【００３７】公開鍵暗号は、キー対(key pairs)として知られる、相互に逆方向の数学的演算(mutually inverse mathematical operations)の非対称対の使用に基づくものである。

【００３８】例えば、Ｅが公開鍵アルゴリズムであるとすると、表記E_k（ｍ）はキーＫを用いたメッセージｍの暗号化を意味する。

【００３９】もし、ＫとK^{-1}がＥのキー対であるならば、E_k（E_{k-1}（ｍ））＝ｍとなる。よって、キーK^{-1}（ここでは秘密鍵という）で暗号化されたメッセージは、キーＫ（ここでは公開鍵という）を適用することにより解読することができる。公開鍵暗号は、キーのビット長が十分大きい（例えば５１２ビット以上）とき、現状では、キー対の一方から他方を算出するには計算上不可能であるという事実に基づくものである。

【００４０】デジタル署名は、公開鍵アルゴリズムおよび一方向ハッシュ関数に基づくことができる。ハッシュ関数は、可変長入力列を受けてこれを、ハッシュ値として知られる一般により小さい出力列に変換する任意の関数である。一方向ハッシュ関数とは、メッセージｍが与えられたとき、ハッシュ値ｃ＝Ｈ（ｍ）を計算することが容易であるが、与えられたハッシュ値ｃを基にｍを算出することが困難であるような関数である。Ｈの出力ビット長が十分大きい（例えば１２８ビット以上）場合、一般にｃからｍを求めることは計算上不可能である。参考としてBruceSchneier, "Applied Cryptography", pp. 29-31, pp.38-39、D.W. Davies, W.L.Price, "The Application of Digital Signitures Based on Public-Key Cryptosystems", Proceedings of the Fifth International Computer CommunicationsConference, October 1980, pp.525-530、およびNational Physical Laboratory Report DNACS 39/80, December 1980を参照されたい。

【００４１】デジタル署名の使用を可能とする方法を以下に説明する。

【００４２】例えば、ＸがＹへメッセージを送りたいとする。メッセージの内容は秘密ではないが、Ｙはそのメ

ッセージがXから発せられたものであること、および、それが第三者により改竄されていないことを確信したい。したがって、Xは公開鍵アルゴリズムEのキー対KおよびK^{-1}を生成する。Xは秘密鍵K^{-1}を保持し、キーKを公衆に公開する。そこで、Xは、メッセージmを作成し、これに対して次のようにしてデジタル的に署名する。

【００４３】１．ｃ＝Ｈ（ｍ）を計算する。ここに、Ｈは既知のハッシュ関数である。

【００４４】２．秘密鍵K^{-1}を用いてＥによりｃを暗号化する。

【００４５】すなわち、デジタル署名＝E_{k-1}（ｃ）デジタル署名は、ここでは、Sig_{k-1}（ｍ）と表されるので、上記式は次のように書ける。

【００４６】Sig_{k-1}（ｍ）＝E_{k-1}（ｃ）

Ｙがメッセージｍを受け取ったとき、Ｙは次の手順により、Ｘの公開鍵Ｋを用いて署名を検証することができる。

【００４７】１．ｃ’＝Ｈ（ｍ）を計算する。

【００４８】２．キーＫを用いてE_{k-1}（ｃ）を復号し、ｃ、すなわちｃ＝E_k（E_{k-1}（ｃ））を求める。

【００４９】３．ｃとｃ’とを比較する。

【００５０】もし、ｃ＝ｃ’であれば、検証は成功であり、そうでなければ検証失敗である。

【００５１】メッセージｍに何らかの変更があった場合に検証失敗となる。なぜなら、この場合、メッセージｃ’のハッシュが変わるからである。また、デジタル署名が偽造された場合にも検証は失敗となる。秘密鍵K^{-1}にアクセスできるのはＸのみであるから、公開鍵Ｋで検証できる正しいデジタル署名を生成できる唯一の人物はＸである。

【００５２】図３に戻り、オリジナルディスク識別子のコピーを用いる上記概説した簡単な場合に上記の保護形成を適用することにより、再生しようとしているディスクの正当性を検証するため、記録装置８内のＣＣＩ生成器１０は、キー対Ｋ，K^{-1}を生成するキー対生成器からの入力端を有する。ＤＳＡやＲＳＡアルゴリズムのような特定のアルゴリズムの生成器を含むキー対生成器ソフトウェアは、広く市販されているものを入手可能であり、例えば、Ｊａｖａ（商標）プログラミング言語で実施できる。例えばＪａｖａＡＰＩは、Java.security.KeyPairGeneratorとして知られているキー対生成クラスを内包している。オリジナルディスクのディスク識別子を表すディスク識別子Ｓｄは、読み出し装置９によりディスク１から読み出され、秘密鍵K^{-1}と、記録装置およびプレーヤの両方で固定の適当な一方向ハッシュ関数Ｈ（ｘ）とを用いてデジタル署名Sig_{K-1}（Ｓｄ）が形成される。

【００５３】適当なハッシュ関数の一例は、前述した"Applied Cryptography"のpp.442-445に記載されたSecure Hash Algorithm (SHA)である。このアルゴリズムは、可変長入力ビット列を受けて、１６０ビットのハッシュを出力する。典型的には、決定されたハッシュ関数の知識は、非開示契約に基づいて記録装置／プレーヤ機器ベンダーに制限される。デジタル署名Sig_{k-1}（Ｓｄ）は、公開キーＫとともにディスク１上に記録される。

【００５４】図５に戻り、プレーヤ１３では、読み出し装置１４は、再生しようとしているディスク１のデータ領域３から公開キーＫおよびSig_{k-1}（Ｓｄ）を読み、識別子領域２からディスク識別子Ｓｐを読む。ＣＣＩ検証器１５は、ハッシュ値Ｈ（Ｓｐ）を算出し、Ｋを用いてSig_{k-1}（Ｓｄ）を解読することによりハッシュ値Ｈ（Ｓｄ）を得る。ＣＣＩ検証器１５は、ついで、これらの２つのハッシュ値を比較する。ＳｄとＳｐが等しければ、再生しようとしているディスクはオリジナルディスクなので、ハッシュ値も同一であり、検証は成功し、再生を許可する信号が再生装置１６へ送られる。ＳｄとＳｐが等しくなければ、再生しようとしているディスクはオリジナルディスクのコピーなので、それらのハッシュ値は異なり、その結果、検証処理は失敗となり、これにより再生装置１６に対して再生を阻止する信号が発せられる。

【００５５】コンテンツ供給者は、秘密キーK^{-1}にアクセスできる唯一の者なので、オリジナルディスクのシリアル番号または他の識別子を正しく暗号化できる唯一の者である。

【００５６】さらに複雑なコピーの管理を可能とするために、コピー管理情報の一部として他の情報を含めることができる。これは、例えば、コピー生成管理が可能なコピー管理フィールドである。

【００５７】図８と図９は、コンテンツ供給者により使用される記録装置２０の他の例の概略構成、および、記録済みコピー防止ディスクの生成に関するステップを説明するためのものである。

【００５８】ステップｓ１７では、キー対生成モジュール２１が署名検証のための公開アルゴリズムのキー対を生成する。ステップｓ１８では、読み出し装置２２がディスク１の読み出し専用部分からＤＶＤディスク１の識別子、例えば、シリアル番号を読み出す。ステップｓ１９では、コピー管理情報（ＣＣＩ）生成器２３が、キー、識別子、およびコピー管理フィールド（ＣＣＦ）データベース２４からのコピー管理フィールドに基づいてデジタル署名を含むコピー管理情報を生成する。このコピー管理フィールドは、コピー自由(Copy-Freely)、ネバーコピー(Never-Copy)、コピーワンス(Copy-Once)、およびノーモアコピー(No-More-Copy)の４つの採りうる値のうちの１つを採ることができる。コピー管理情報を作成するための実際の情報について以下に詳述する。ステップｓ２０では、記録モジュール２５が、ＤＶＤディスク１に書かれるべきデータをデータアーカイブ２６か

ら読み出し、このデータとＣＣＩ生成器２３からのコピー管理情報とをＤＶＤディスク１に書き込むことにより、コピー防止化された記録済みＤＶＤディスクが完成する。

【００５９】ＤＶＤプレーヤの概略構成および機能については、図５および図６により既に説明した。

【００６０】図１０は、消費者が記録可能ディスク上にデータを記録するために用いる本発明の記録装置３０の構成を示す。図１０および図１１において、ステップｓ２２で、入力信号処理モジュール３１は、前述したようにディスクプレーヤ１３からコピー管理情報および記録対象のデータを受け取り、これらをＣＣＩ検証器モジュール３２およびＣＣＩ生成器３３へ送る。ステップｓ２３では、ＣＣＩ検証器３２がコピー管理情報を検証しようとする。ＣＣＩ検証器３２は、プレーヤ１３内のＣＣＩ検証器１５と同じ検証機能を実行する。もし、プレーヤと記録装置が単一ユニットとして実現されている場合、検証器３２は同じ回路または同じソフトウェア機能により実現される。しかし、記録装置３０がプレーヤ１３とは別のユニットである場合、ＣＣＩ検証器３２は二重チェック機能として実装され、プレーヤに検証機能を与える。このプレーヤにはコピー保護機能は含まなくてよい。

【００６１】この段階で検証が失敗したら（ｓ２３）、制御はステップｓ２９へ移行し、新たなディスク上へのデータの記録は阻止される。検証が成功であれば、制御はステップｓ２４へ進み、ここで、例えばコピーフリーフラグの存在により、データが自由にコピーできることをコピー管理フィールドが示しているか否かをＣＣＩ検証器３２が判定する。もしデータが自由にコピーできるならば、制御はステップｓ２８へ移行し、ここで、記録モジュール３４がコピー管理情報およびデータを新たなディスク３５へ記録する。ステップｓ２４でもしデータが自由にコピーできないことをコピー管理情報が示していれば、制御はステップｓ２５へ移行し、ここで、例えばコピーワンスフラグの存在により、データが１回だけコピーできることをコピー管理フィールドが示しているか否かをＣＣＩ検証器３２が判定する。もし、フラグがコピーワンスフラグでなければ、ネバーコピーかノーモアコピーフラグがセットされていることになり、制御はステップｓ２９へ進み、ここで記録が阻止される。一方、ステップｓ２５で、コピーワンスフラグがセットされていることをコピー管理情報が示していたら、制御はステップｓ２６へ進み、ここで、読み出し装置２６が、新たなディスク３５の媒体識別子をそのディスクの読み出し専用部分から読み出し、この識別子をＣＣＩ生成器３３へ送る。ステップｓ２７では、ＣＣＩ生成器はコピー管理フィールドをコピーワンスからコピーノーモアに変え、記録モジュール３４でディスク３５に記録されるべき新たなコピー管理情報を生成する。この新たなコピー管理情報の性質(nature)については後に詳述する。

【００６２】オリジナルディスクに書き込まれるコピー管理情報の厳密な性質は、コンテンツ供給者が達成したい保護のレベルに依存する。例えば、供給者は、例えばそのＤＶＤオーディオディスクの内容を全くコピー不可能としようとするかもしれない。あるいは、供給者はオリジナルのバックアップコピーを生成する能力を顧客に対して与えるが、それ以上のコピーの生成能力は与えたくないかもしれない。これらの目的を達成可能な方法については、次のような表記を用いて以下に説明する。

【００６３】ＩＤはコンテンツ供給者を識別する情報である。これは、供給者の名称、コンテンツの名称、生成日、等を含みうる。ＣＣＦは、上述したように、コピー自由、ネバーコピー、コピーワンス、ノーモアコピーの値を採りうるコピー管理フィールドを表す。ＡおよびＡ'は、供給者依存情報ＩＤおよびＣＣＦを一緒にグループ化するのに便利な表記として用いる。例えば、Ａ＝ＩＤ｜ＣＣＦ　かつ　Ａ'＝ＩＤ｜ＣＣＦ'の如くである。ここに、ＣＣＦ'は新たなディスク上への記録時にコピー管理フィールドの値の変化を表す。Ｓｄ，Ｓｃ，Ｓｐは、ディスクの読み出し専用部分に印刷されたディスク識別子である。したがって、これらの識別子は顧客によって変更されない。Ｓｄは、オリジナルディスク識別子を表し、Ｓｃは、オリジナルディスクが合法的にコピーされうるディスクのディスク識別子を表し、Ｓｐは、再生しようとしているディスクのディスク識別子を表す。Ｓｐは、Ｓｄ，Ｓｃの値を採ることができる。その場合、オリジナルディスクおよびその合法的コピーがそれぞれ再生されていようとしていることになる。

【００６４】K_AおよびK_{A-1}は、コンテンツ供給者のデジタル署名のためのキー対である。K_MおよびK_{M-1}は、例えば、コピーはオリジナルからのみ可能で、オリジナルのコピーからは不可能とすることを保証するＣＧＭＳスキームを実現するために必要なデジタル署名のためのキー対である。

【００６５】図８および図１２において、コンテンツ供給者が、バックアップコピーの作成も含めてオリジナルディスクからのあらゆる複製を禁止することを望む場合、ステップｓ３０で、ＣＣＦフラグをネバーコピーにセットする。ステップｓ３１では、キー対発生モジュール２１は、第１の例について上述したキー対K_AおよびK_{A-1}を生成する。次に、読み出し装置２２がディスク１の読み出し専用部分からＳｄを読み出し（ｓ３２）、ステップｓ３３でＣＣＩ生成器２３がデジタル署名$Sig_{K_{A-1}}(Sd,A)$を計算する。この場合のコピー管理情報は$Sig_{K_{A-1}}(Sd,A)$とK_Aとからなる。記録モジュール２５は、次に、データアーカイブ２６からデータを読み出し（ｓ３４）、ステップｓ３５で、ＣＣＩ生成器２３からのコピー管理情報とともにデータをディスク１に書き込む。

【００６６】図５および図１３において、上記データで

符号化されたＤＶＤディスク１がＤＶＤプレーヤ１３内に挿入されると、ステップｓ４０で、読み出し装置１４がディスク１の読み出し専用部分２からSpを読み出す。読み出し装置１４は、また、データ領域３からコピー管理情報、すなわちＡ，K_Aおよび$SigK_{A-1}(Sd,A)$を読み出す。ＣＣＩ検証器１５は、そこで、ステップｓ４１において、Ｓｄ，Ａ，K_Aを用いて$SigK_{A-1}(Sd,A)$を検証する。もし、検証が成功すれば、制御はステップｓ４２へ移行し、ここで、データが再生される。そうでなければ、制御はステップｓ４３へ進み、ここでデータの再生が阻止される。この例の動作を更に説明するために、以下に検証処理を詳細に説明する。

【００６７】ディスクの識別子領域２から読み出されたSpおよびディスクのデータ領域３から読み出されたＡを認識することにより、１方向ハッシュ関数Ｈを用いて関数ｃ’を計算することができる。すなわち、ｃ’＝Ｈ（ｍ）、ここにｍ＝（Ｓｐ，Ａ）である。したがって、ｃ’＝Ｈ（Ｓｐ，Ａ）となる。

【００６８】関数Ｈは、関数ｃ＝Ｈ（Ｓｐ，Ａ）を生成するために記録装置２０で用いられたものと同じ関数である。この関数は、ディスク１のデータ領域３から読み出された公開キーK_Aを用いて、$SigK_{A-1}(Sd,A)$を復号化することにより得られる。

【００６９】もし、ｃ＝ｃ’、すなわち、Ｈ（Ｓｄ，Ａ）＝Ｈ（Ｓｐ，Ａ）ならば、これは、ＡとSpの両方ともが記録時から不変であり、特に、Ｓｐ＝Ｓｄ、すなわち、再生しようとするディスク上のシリアル番号と、データが記録されたディスクのシリアル番号とが同じであることを示している。シリアル番号が一意であるとすると、このことは、再生しようとしているディスクがオリジナルディスクであり、よって、それに含まれるデータの再生が許可されることを示している。検証が失敗に終われば、再生しようとしているディスクはコピーであると推測され、その再生が阻止される。

【００７０】図８および図１４において、コンテンツ供給者がオリジナルディスクからのみバックアップコピーの作成する機能を与えたい場合、ステップｓ５０で、コピー管理フィールドをコピーワンスにセットする。ステップｓ５１では、キー対生成モジュール２１がキー対K_AおよびK_{A-1}とともにK_MおよびK_{M-1}を生成する。読み出し装置２２は、ディスク１の読み出し専用部分からＳｄを読み出し（ｓ５２）、ステップｓ５３で、デジタル署名$SigK_{A-1}(Sd,A,K_M)$を計算する。そこで、記録モジュール２５はデータアーカイブ２６からデータを読み出し（ｓ５４）、ステップｓ５５でディスク１に対してデータとともにＣＣＩ生成器２３からのコピー管理情報を書き込む。このコピー管理情報は、Ａ，K_A，K_M，K_{M-1}および$SigK_{A-1}(Sd,A,K_M)$を含む。

【００７１】図５および図１５において、上記データで符号化されたＤＶＤディスク１がＤＶＤプレーヤ１３内に挿入されると、ステップｓ６０で、読み出し装置１４がディスク１の読み出し専用部分２からSpを読み出す。読み出し装置１４はまた、ディスク１のデータ領域からコピー管理情報、すなわち、Ａ，K_A，K_M，K_{M-1}および$SigK_{A-1}(Sd,A,K_M)$を読み出す。ＣＣＩ検証モジュール１５は、先に詳述したように、Ｓｄ，Ａ，K_MおよびK_Aを用いてデジタル署名$SigK_{A-1}(Sd,A,K_M)$を検証する。検証が成功であれば、制御はステップｓ６２へ進み、データが再生される。そうでなければ、制御はステップｓ６３へ進み、データの再生が阻止される。

【００７２】オリジナルディスクのバックアップコピーの作成は許容されるので、図１０に示した記録装置３０の詳細動作は、図１６のフローチャートで示される。図１０および図１５も参照し、ステップｓ７０およびｓ７１は、再生装置により実行されるようなステップｓ６０およびｓ６１と同じである。もし検証が失敗に終われば、それ以降の処理はステップｓ７２で終了する。検証処理内にK_Mを含める目的は、K_Mが偽造されたものではないことを確かめるためである。なぜなら、キー対K_MおよびK_{M-1}の両部分が含まれており、よって、オリジナルディスク上で潜在的な侵害者に利用可能だからである。検証手続が成功であれば、ステップｓ７３において、読み出し装置３６が書き込み先ディスク３５の読み出し専用部分からScを読み出す。ＣＣＩ生成器３３は、Ａのコピー管理フィールドをコピーワンスからノーモアコピーへ変更し、これをＡ’として保存する（ｓ７４）。ＣＣＩ生成器３３は、ついで、デジタル署名$SigK_{M-1}(Sc,A')$を計算し（ｓ７５）、ステップｓ７６で、書き込み先ディスク３５のデータ領域３に、Ｓｄ，Ａ，K_M，K_A，$SigK_{A-1}(Sd,A,K_M)$，Ａ’および$SigK_{M-1}(Sc,A')$を書き込む。

【００７３】図５および図１７において、ノーモアコピーフラグが付されたディスクからデータを再生するには、ステップｓ８０で、読み出し装置１４がディスク３５の読み出し専用部分２からSpを読み出す。読み出し装置１４はまた、そのディスクのデータ領域３からコピー管理情報、すなわち、Ｓｄ，Ａ，K_M，K_A，$SigK_{A-1}(Sd,A,K_M)$，Ａ’および$SigK_{M-1}(Sc,A')$を読み出す（ｓ８１）。ＣＣＩ検証器１５は、ついで、Ｓｄ，Ａ，K_Mを用いてデジタル署名$SigK_{A-1}(Sd,A,K_M)$を検証する（ｓ８２）。このステップは、検証処理の第２部分で用いたキーK_M自身が偽造されたものでないことを検証するものである。この検証が失敗すれば、再生は阻止される（ステップｓ８５）。検証が成功であれば、次にステップｓ８３で、ＣＣＩ検証モジュール１５が、Ｓｐ，Ａ’およびK_Mを用いて第２のデジタル署名$SigK_{M-1}(Sc,A')$の検証を行う。もし、Ｓｐ＝Ｓｃならば、このステップは、コピーされたディスク自体がコピーされたものではないことを示し、よって、第２世代コピーの再生を阻止する。検証が成功であれば、再生装置１７はデータを再生し

（ｓ８４）、そうでなければ再生は阻止される（ｓ８５）。

【００７４】本発明による方法は、記憶媒体に対して一意なまたはほぼ一意な識別子を関連づけることができる任意の汎用デジタル記録システムに利用することができることが理解されよう。この記憶媒体には、例えば、識別子の不可変記憶のためのＲＯＭ領域部分を有するスマートカードＲＡＭメモリを含む。

【００７５】また、公開鍵アルゴリズムに基づく方法について詳細に説明したが、デジタル署名を行うたの手段を排除するものではない。

【図面の簡単な説明】

【図１】　本発明によるＤＶＤディスクの概略図である。

【図２】　図１のディスクを製造するために使用される装置の概略ブロック図である。

【図３】　コピー防止されたディスクを作成するためにコンテンツ供給者により使用されるべき記録装置の一例を示す概略ブロック図である。

【図４】　図３の記録装置の動作を示すフロー図である。

【図５】　本発明によるＤＶＤプレーヤの概略ブロック図である。

【図６】　図５のプレーヤの動作を示すフロー図である。

【図７】　コピー管理情報の所定の例に基づく、図３の記録装置および図５のプレーヤの詳細な動作を示すフロー図である。

【図８】　本発明の他の例によるコンテンツ供給者により使用されるべき記録装置の概略ブロック図である。

【図９】　図８の記録装置の動作を示すフロー図である。

【図１０】　消費者装置に利用されるべき本発明によるデータ記録装置の概略ブロック図である。

【図１１】　図１０の記録装置の動作を示すフロー図である。

【図１２】　オリジナルディスクのコピーが許されない場合の、図８の記録装置の詳細動作を示すフロー図である。

【図１３】　再生しようとしているディスクが図１２に示した記録動作に従って記録されている場合の図５のプレーヤの詳細動作を示すフロー図である。

【図１４】　オリジナルディスクからの１回のコピー生成が許される場合の、図８の記録装置の詳細動作を示すフロー図である。

【図１５】　再生しようとしているディスクが図１４の記録動作に従って記録されている場合の、図５のプレーヤの詳細動作を示すフロー図である。

【図１６】　記録中のデータ自体が図１４の記録動作に従って記録されていた場合の図１０の記録装置の詳細動作を示すフロー図である。

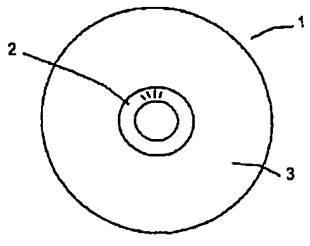
【図１７】　再生しようとしているディスクが図１６に示した記録動作に従って記録されている場合の、図５のプレーヤの詳細動作を示すフロー図である。

【符号の説明】

１　ＤＶＤディスク
２　識別子領域
３　データ領域
４　未記録（ブランク）ＤＶＤディスク

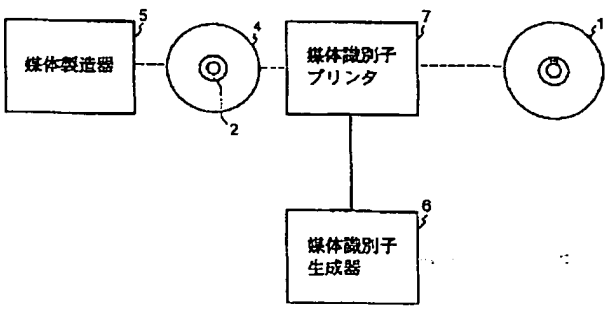
【図１】

図1



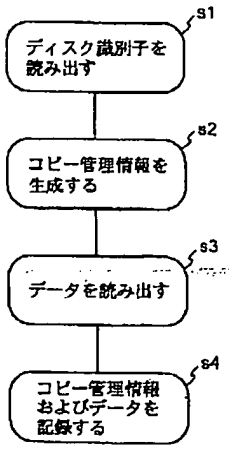
【図２】

図2



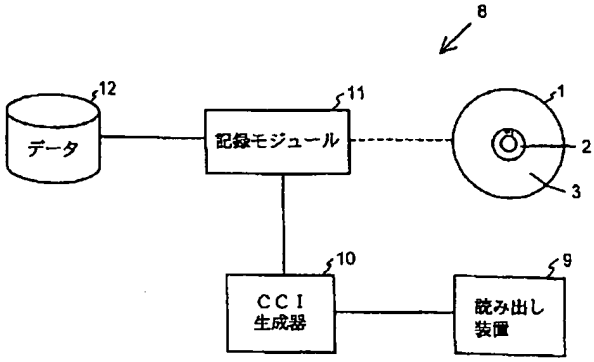
【図４】

図4



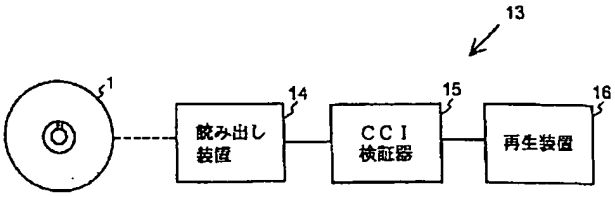
【図3】

図3



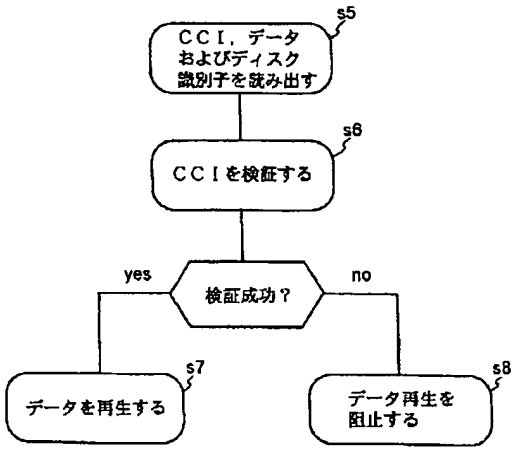
【図5】

図5



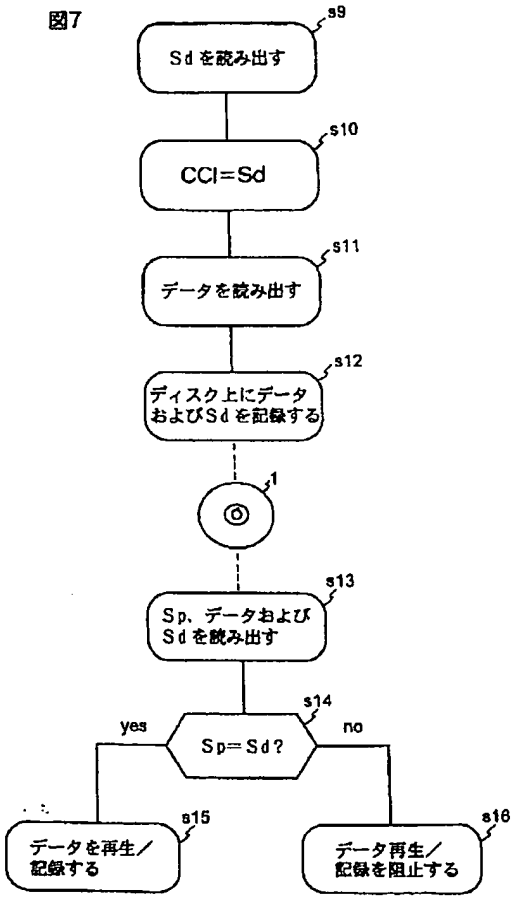
【図6】

図6



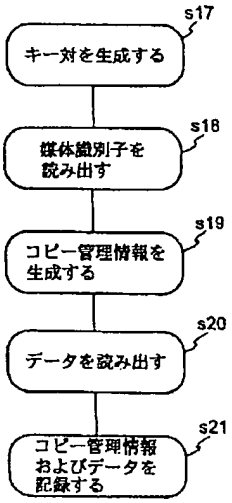
【図7】

図7



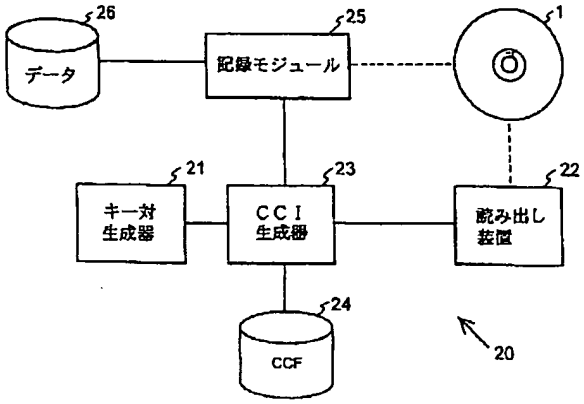
【図9】

図9



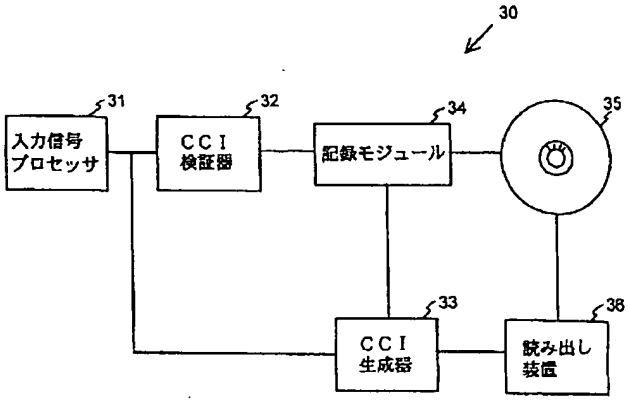
【図8】

図8



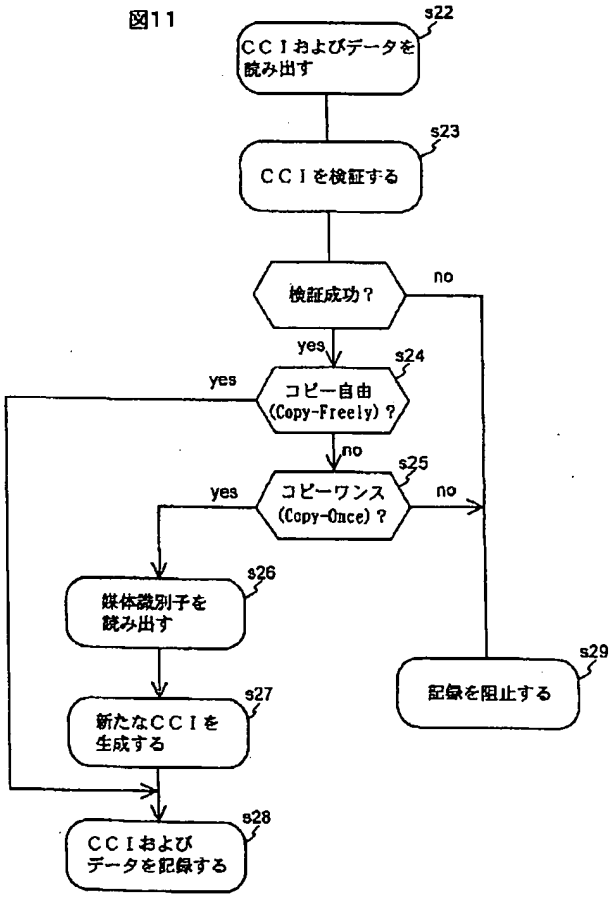
【図10】

図10



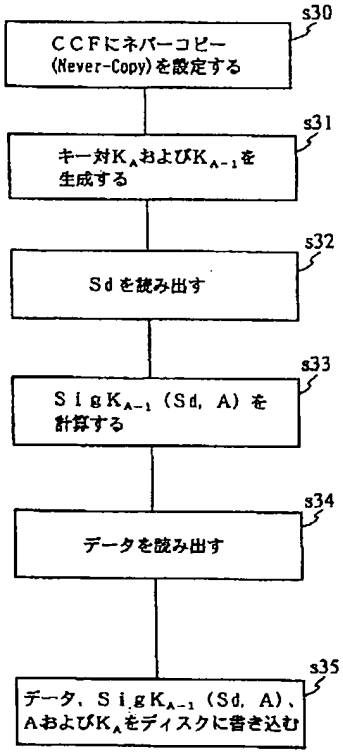
【図11】

図11



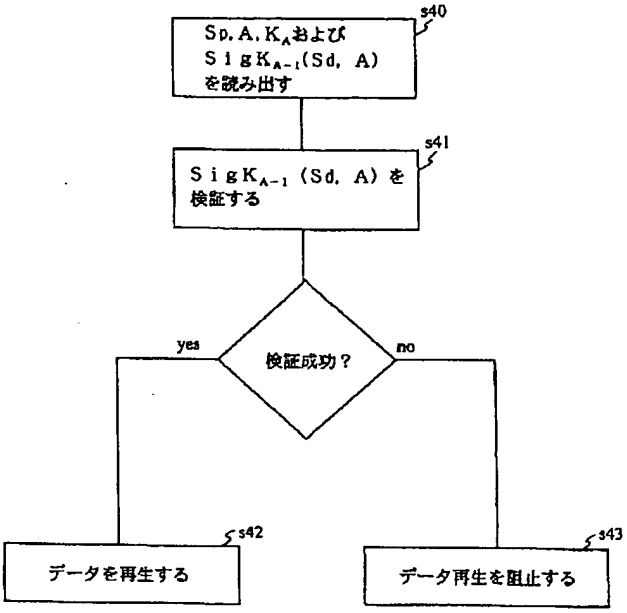
【図12】

図12



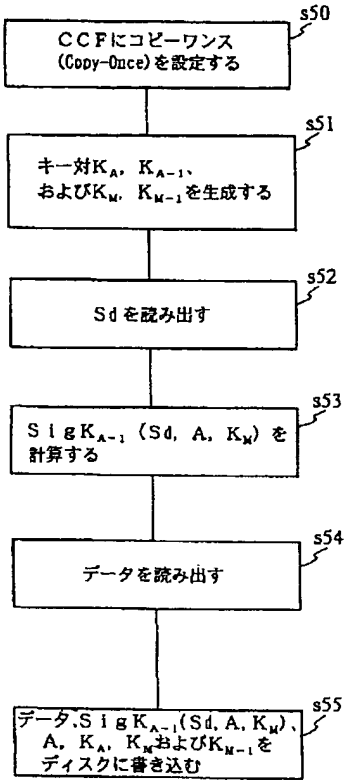
【図13】

図13



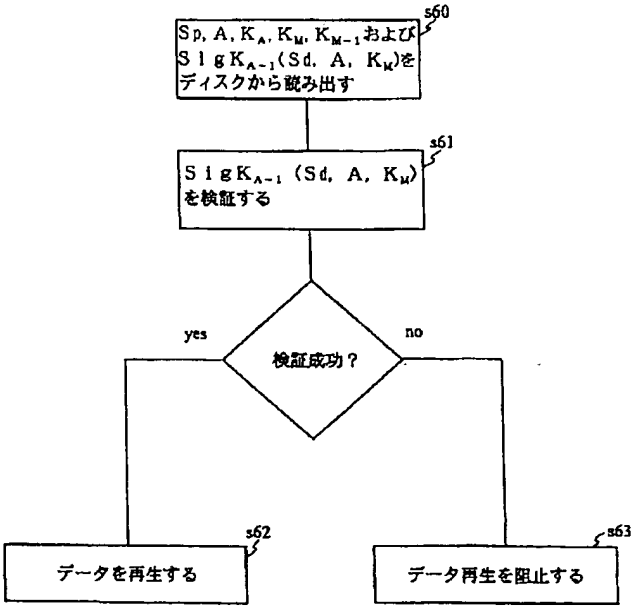
【図14】

図14



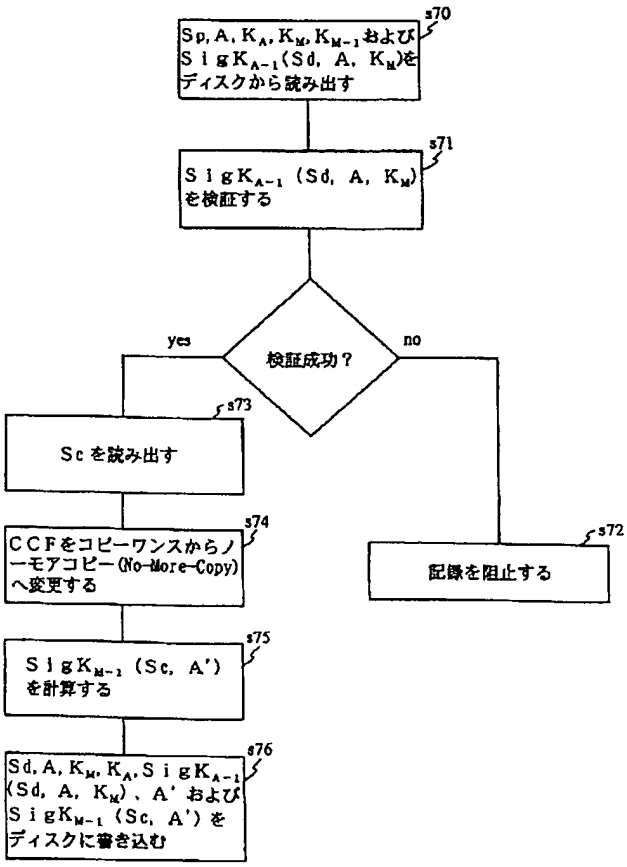
【図15】

図15



【図16】

図16



【図17】

図17